Last time: Lemma: \( f \in \mathbb{Z}[x] \), if \( a \) is a simple root of \( f \mod p \), then \( \exists a' \in \mathbb{Z}_p \) with \( f(a') = 0 \) and \( a = a' \mod p \).

\underline{Hensel's Lemma:} Suppose \( f \in \mathbb{Z}_p[x] \) is monic. Let \( \overline{f} \in \mathbb{F}_p[x] \) be its reduction mod \( p \). If \( \overline{f} \) factors into \( g_0 h_0 \) with \( g_0 \) and \( h_0 \) monic and not prime (in \( \mathbb{F}_p[x] \)), then \( \exists \) monic \( g, h \in \mathbb{Z}_p \) with \( f = gh \) and \( \overline{g} = g_0 \) and \( \overline{h} = h_0 \).

Moreover, \( g \) and \( h \) are unique and \( (g, h) = \mathbb{Z}_p[x] \).

Lemma from last time is special case of \( g_0 \) linear; will omit proof, which has a similar inductive approach.

Usefulness of \( \mathbb{Z}_p \) in computations, e.g. factoring polynomials.

\[ \text{On to number fields...} \]
\[ K, \beta \rightarrow K_{\beta} \text{ "local field"} \]
\[ \text{global field} \]

Def: Two valuations \( \nu_1 \) and \( \nu_2 \) on \( K \) are equivalent if
\[ \begin{array}{l}
0 \nu_2 = \nu_1^a \text{ for some } a > 0. \\
|a|_1 < 1 \Rightarrow |a|_2 < 1 \\
\text{They define the same topology on } K 
\end{array} \]

Lemma: These are equivalent cond.
$K$ a number field.

Place or Prime of $K$: an equivalence class of valuations.

**Thm:** There is exactly one place of $K$ for each

1. real embedding $\tau: K \to \mathbb{R}$, namely $|k|_{\tau} = |\tau(k)|$.
2. pair of complex embeddings $\sigma, \bar{\sigma}: K \to \mathbb{C}$, namely $|k| = |\sigma(k)|^2$.
3. prime ideal $\mathfrak{p}$ of $O_K$:

   $$|k|_{\mathfrak{p}} = |N(\mathfrak{p})|^{-m}$$

   where $(k) = \mathfrak{p}^m \mathfrak{q}$ with
   
   $\mathfrak{q}$ coprime to $\mathfrak{p}$.

**Notes:**
1+2 are the infinite places (or primes)
3 the finite places

**clm:** it's not really a valuation, but just ignore it.

**Product Formula:**

$$\prod_{v \text{ place of } K} |k|_v = 1 \text{ for any } k \neq 0 \text{ in } K.$$

**Ex:** $K = \mathbb{Q}(i)$ in $\mathbb{Q}(i)$

$k = (1+i)^3$

So

$$|k|_v = \begin{cases} 
72 = 2^3 \cdot 3^2 & \text{if } v = \infty \\
2^{-3} & \text{if } v = (1+i) \\
3^{-2} & \text{if } v = (3) \\
1 & \text{otherwise}
\end{cases}$$
In a place \( v \), let \( K_v \) denote its completion w.r.t. \( \nu_v \). Equivalently:

\( a \) if \( v \) is an infinite place, \( K_v = \mathbb{R} \)

\( b \) if \( v \) is a finite place coming from \( \beta \), then take

\[ O_v = \lim \frac{O_k}{\beta^n} \quad \text{and} \quad K_v = \text{field of fractions of } O_v \]

**Example:** \( K = \mathbb{Q}(i) \)

\( v = (3) \): On \( \mathbb{Q} \) we have \( |r|_v = \left(\frac{1}{3}\right)^m \) where \( r = 3^m \frac{x}{y} \) with \( x, y \) coprime to 3. This is equivalent to the usual 3-adic valuation. So

\[ \mathbb{Q}_3 \subseteq K_{(3)} \quad \text{in fact} \quad K_{(3)} = \mathbb{Q}_3(i) \quad \text{i.e. a finite extension of } \mathbb{Q}_3. \]

\( O_{(3)} \) like \( \mathbb{Z}_3 \) except \( O_{(3)}/\text{unique prime ideal} \equiv O_K/3 \equiv \mathbb{F}_9 \).

\( v = (2+i) \): In this case, \( K_{(2+i)} \cong \mathbb{Q}_5 \)

**Point:** \(-1\) is already a square in \( \mathbb{Q}_5 \) as \( x^2 + 1 \equiv (x+2)(x+3) \mod 5. \)

\( v = (1+i) \): The tricky ramified case.

\[ \text{Have } K_{(1+i)} \neq \mathbb{Q}_2 \text{ since } x^2 + 1 \equiv 0 \mod 4 \text{ has no solutions. However, } (\mathbb{Z}_2)^* \text{ isn't prime.} \]
Global field: a number field $K$ (or a finite extension of $\mathbb{F}_p(T)$).

Local field: $K_v$ for same place $v$.

Local-to-global principles:

A quadratic form $g : K^n \to K$ is $g(x) = \langle x, x \rangle$ for some symmetric bilinear form $\langle , \rangle : K^n \times K^n \to K$.

[Note: $g$ determines $\langle , \rangle$ by $\frac{1}{2} \{ g(x+y) - g(x) - g(y) \}$,]

Thus: $g$ a quad. form on $\mathbb{Q}^n$. Then $\exists x \in \mathbb{Q}^n$ with $g(x) = 0$ if and only if $\forall p \in \mathbb{Q}_p \cap \mathbb{Q}^n$ with $g(x_p) = 0$.

"$g$ reps 0 globally iff it does at every local place."

Why this is good: Local fields are "large" so there are few distinct quadratic forms over them. E.g., at the infinite place $\mathbb{R}$, any form $x^2 + x_k^2 - (x_{k+1}^2 + \cdots + x_n^2)$ is equal to one of the form $x^2 + x_k^2$. 